BESKRIVNING AV PERSONUPPGIFTSHANTERING

Elisabeth Bexell

BRIZAD BEHANDLINGSKONSULT AB

1. Inledning

Det här dokumentet beskriver regler och riktlinjer för hantering av personuppgifter inom Brizad Behandlingskonsult AB i fortsättning kallat ”företaget” samt ”personuppgiftsansvarig”. Dokumentet beskriver även den handlingsplan som är beslutad för att företaget ska uppnå GDPR Compliance.

2. Kontaktuppgifter till personuppgiftsansvarig

Brizad Behandlingskonsult AB
Elisabeth Bexell
Box 1087
824 12 Hudiksvall
Växel: 0650-59 53 30
Epost: info@brizad.se

3. Vad uppgifterna används till

Samtliga personuppgifter som företaget hanterar är nödvändiga för att fullgöra avtal , vidta åtgärder eller utföra uppgifter av allmänt intresse samt för att fullgöra företagets rättsliga skyldigheter. Behandlingen kan också vara nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade. I förekommande fall har vi både skriftligt och muntligt samtycke för personuppgiftsbehandlingen.

4. Övergripande hantering

Företagets samtliga register innehållande personuppgifter ska vara registrerade i ett ändamålsenligt system. Arbetet är pågående och rutinbeskrivning utarbetas.

5. Mailhantering

Vi skickar inga känsliga personuppgifter i mail, ex religiös åskådning, politiska åsikter eller om någons hälsa. Vi sparar bara mail så länge det är relevant att spara utifrån verksamhetens perspektiv och vi går igenom inkorg och mappar minst 4 ggr/år och tar bort mail som inte behöver sparas. Detta informeras personal om och ansvaret för borttaget ligger på varje medarbetare.

6. Information om GDPR

I alla våra utskick och kommunikation med kunder, leverantörer, samarbetspartners och uppdragsgivare, oavsett media, så finns hänvisning till hur vi hanterar GDPR. I mailutskick, ex nyhetsbrev och marknadsföring så finns tydlig information om avregistrering och information om var på hemsidan det finns mer information.

Med Tillämpliga bestämmelser avses bestämmelser och praxis hänförlig till dataskyddsförordningen, nationell kompletteringslagstiftning till dataskyddsförordningen, tillsynsmyndigheters (inkl. Europeiska dataskyddsstyrelsen) föreskrifter, yttranden och kommissionens rättsakter på personuppgiftsområdet.

7. Lagring och gallring

Personuppgiftsansvarig ska säkerställa att de grundläggande principerna för behandling av personuppgifter efterlevs, däribland särskilt lagringsminimering. Personuppgiftsansvarig ansvarar för att personuppgifter som inte längre behövs för ändamålet gallras. Personuppgiftsansvarig ska upprätta rutiner för hur personuppgifter gallras, vilka personuppgifter som gallras och hur ofta gallring sker.

8. Överföring av personuppgifter

Personuppgiftsansvarig får inte överföra några personuppgifter till en stat utanför EU-området eller till en stat som inte omfattas av undantagen till förbud mot överföring till tredje land enligt Tillämpliga bestämmelser. Förbudet omfattar även service, teknisk support, underhåll, utveckling och liknande tjänster av systemet.

9. Vidta tekniska och organisatoriska åtgärder

När företaget behandlar personuppgifter vidtas lämpliga tekniska och organisatoriska åtgärder för att uppfylla kraven i förordningen både när beslut fattas om hur behandlingen ska genomföras och under hela den fortsatta behandlingen. Vilka åtgärder som behövs beror på uppgifternas art, omfattning och syfte med behandlingen liksom vilka risker för enskildas rättigheter och friheter som behandlingen kan innebära. Exempel på åtgärder som används är

- pseudonymisering och kryptering av personuppgifter
- att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och tjänsterna
- att säkerställa återställning av tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident
- ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

10. Utvärdera risker

Personuppgiftsansvarig ska utvärdera riskerna med behandlingen och vidta lämpliga åtgärder för att minska dem. Åtgärderna bör säkerställa en lämplig säkerhetsnivå, inbegripet konfidentialitet, med beaktande av den senaste utvecklingen och genomförandekostnader i förhållande till riskerna och vilken typ av personuppgifter som ska skyddas.

11. Vidta säkerhetsåtgärder

Personuppgiftsansvarig ska vidta åtgärder för att säkerställa att varje fysisk- och juridisk person som utför arbete under Personuppgiftsansvarigs överinseende, och som får tillgång till personuppgifter, endast behandlar dessa på instruktion från den Personuppgiftsansvarige.

Säkerhetsåtgärderna omfattar såväl tekniska som organisatoriska åtgärder. Omfattningen av åtgärderna ska vidtas med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter. Den säkerhetsnivå som ska säkerställas ska vara lämplig i förhållande till riskerna.

12. Tillräcklig kunskap och utbildning

Personuppgiftsansvarig ansvarar för att varje fysisk person som har tillgång till personuppgifterna som behandlas har tillräckliga kunskaper och utbildning för att på ett säkert och ändamålsenligt sätt behandla personuppgifterna.

13. Ändamålsenliga sekretessåtaganden

Personuppgiftsansvarig ska tillse att samtliga anställda, konsulter och övriga som Personuppgiftsansvarig svarar för och som behandlar personuppgifter är bundna av ett ändamålsenligt sekretessåtagande samt att de är informerade om hur behandling av personuppgifterna får ske.

14. Information till personer med åtkomst

Personuppgiftsansvarig ansvarar för att de personer som har åtkomst till personuppgifterna är informerade om hur de får behandla personuppgifterna i enlighet med de dokumenterade instruktionerna från Personuppgiftsansvarige.

15. Vidta skadebegränsande åtgärder

Vid en misstänkt eller upptäckt personuppgiftsincident ska Personuppgiftsansvarig omedelbart undersöka incidenten och vidta lämpliga åtgärder för att mildra dess potentiella negativa effekter.

Beskrivning av personuppgiftsincident: Personuppgiftsansvarige skall beskriva personuppgiftsincidenten inom 48 timmar. En sådan beskrivning ska åtminstone innehålla

- beskriva personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs
- förmedla namnet på och kontaktuppgifterna för dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas
- beskriva de sannolika konsekvenserna av personuppgiftsincidenten
- beskriva de åtgärder som Personuppgiftsansvarigt har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.

Om och i den utsträckning det inte är möjligt att tillhandahålla informationen samtidigt, får informationen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.

16. Rutiner vid gallring

Gallring av personuppgifter sker löpande och det görs alltid vid begäran om avregistrering eller när företaget upptäcker att det är uppgifter som inte behövs sparas utifrån tjänstens behov. Det kan vara personer som slutat sin anställning, verksamheter som upphört eller liknande.

17. Versionshantering

Version	Datum	Författare	Beskrivning
Version 1.0	2018-05-09	Anders Berglund	Ursprunglig
Version 1.05	2018-05-15	Anders Berglund	Omformuleringar och rättelser